


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)


[Advanced Search](#)  
[Preferences](#)

The "AND" operator is unnecessary -- we include all search terms by default. [\[details\]](#)

**Web** Results 1 - 10 of about **398** for **"hash" and "message authentication code" and "compression function"**

### The HMAC papers

HMAC is a **hash** function based **message authentication code** that was designed to meet ... Moreover they use the **hash** function (or its **compression function**) as a ...

[www.cs.ucsd.edu/users/mihir/papers/hmac.html](http://www.cs.ucsd.edu/users/mihir/papers/hmac.html) - 7k - [Cached](#) - [Similar pages](#)

### [PDF] The Keyed-Hash Message Authentication Code (HMAC)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... **Message Authentication Code** MAC **Message Authentication Code** NIST National ... function, H, with another **hash** function, H ... results of the **compression function** on the B ...

[csrc.nist.gov/publications/fips/fips198/fips-198a.pdf](http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf) - [Similar pages](#)

### [PDF] Draft FIPS: The Keyed-Hash Message Authentication Code (HMAC)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... Conceptually, the intermediate results of the **compression function** on the B ... 71] American Bankers Association, **Keyed Hash Message Authentication Code**, ANSI X9.71 ...

[csrc.nist.gov/publications/fips/dfips-HMAC.pdf](http://csrc.nist.gov/publications/fips/dfips-HMAC.pdf) - [Similar pages](#)

### [PDF] VLSI IMPLEMENTATION OF THE KEYED-HASH MESSAGE AUTHENTICATION CODE ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... Each block  $X_i$  serves as input to the **compression function**  $h$ , which ... message  $x$ . 3 PROPOSED SYSTEM The **Keyed-Hash Message Authentication Code (HMAC)** Standard [3 ...

[www.vlsi.ee.upatras.gr/~gselimis/papers/2003/ICECS\\_2003.pdf](http://www.vlsi.ee.upatras.gr/~gselimis/papers/2003/ICECS_2003.pdf) - [Similar pages](#)

### Alan Kaminsky -- Cryptographic One-Way Hash Functions

... **Compression Function**. ... A **message authentication code (MAC)** is like a one-way **hash** function, except you need a secret authentication key to compute the MAC: ...

[www.cs.rit.edu/~ark/lectures/onewayhash/onewayhash.shtml](http://www.cs.rit.edu/~ark/lectures/onewayhash/onewayhash.shtml) - 7k - [Cached](#) - [Similar pages](#)

### [PPT] Crypto Hash

File Format: Microsoft Powerpoint 97 - [View as HTML](#)

... 6. **Message Authentication Code**. ... Cryptographic **hash** functions are fast, freely available and not subject to ... For key  $K = (K_1, K_2)$ ,  $f_K$  - **compression function** and  $F_K$  ...

[www.ccs.neu.edu/home/gassko/Courses/CSU900/lectures/15v1.ppt](http://www.ccs.neu.edu/home/gassko/Courses/CSU900/lectures/15v1.ppt) - [Similar pages](#)

### [PDF] Microsoft PowerPoint - 15v1.ppt

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... 6 **Message Authentication Code** • MAC is a triple of PPT ... **Hash Functions for MACs** • Cryptographic **hash** functions are ...  $K_1, K_2$ ,  $f_K$  - **compression function** and  $F_K$  ...

[www.ccs.neu.edu/home/gassko/Courses/CSU900/lectures/15v1.pdf](http://www.ccs.neu.edu/home/gassko/Courses/CSU900/lectures/15v1.pdf) - [Similar pages](#)

### Security Forums Dot Com :: View topic - How does this work : VPN ...

... has demonstrated collision-susceptibility in its **compression function**. ... HMAC is a **message authentication code** scheme involving the ... of a keyed **hash** function; MD5 ...

[www.security-forums.com/forum/viewtopic.php?p=109288](http://www.security-forums.com/forum/viewtopic.php?p=109288) - 38k - [Cached](#) - [Similar pages](#)

### [PDF] Microsoft PowerPoint - HASHFUN

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... adversary, given a set of message/hash pairs, ( $x_i$  ... the full block length of the **compression function** used in h. 4/29/2004 17 **Message Authentication Code** 4/29 ...

[www.cs.mu.oz.au/448/HASH.6.pdf](http://www.cs.mu.oz.au/448/HASH.6.pdf) - [Similar pages](#)

[SecureProgramming.com](http://SecureProgramming.com)

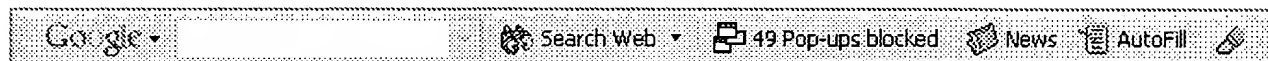
... MAC. See **Message Authentication Code**. ... block cipher into a cryptographic one-way **hash function** ... method for turning a collision-resistant **compression function** into a ...

[www.secureprogramming.com/?action=browse&feature=glossary&letter=M](http://www.secureprogramming.com/?action=browse&feature=glossary&letter=M) - 15k - [Cached](#) - [Similar pages](#)

Google

Result Page: 1 2 3 4 5 6 7 8 9 10 [Next](#)

Free! Get the Google Toolbar. [Download Now](#) - [About Toolbar](#)



"hash" and "message authentication" [Search](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google